PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-339153
(43)Date of publication of application : 08.12.2000

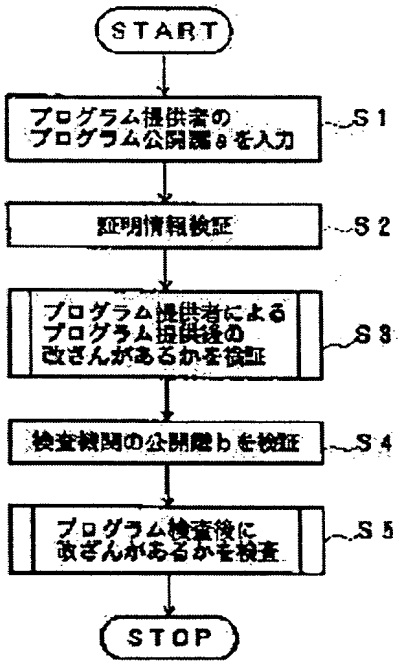
(51)Int.CI. G06F 9/06

(21)Application number : 11-145517
(22)Date of filing : 25.05.1999

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : SUZUKI KATSUHIKO
NIWANO EIICHI
CHIBA NOBUHIRO
HOSODA YASUHIRO

(54) METHOD AND DEVICE FOR VERIFYING PROGRAM AND STORAGE MEDIUM STORING PROGRAM VERIFICATION PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To verify that a supplied program safely operates by permitting an inspection organization to decide whether the program executed after the inspection of the operation of the program is falsified or not.
SOLUTION: When an open key (c) for verifying information is given (S1), proof information (a) is verified by the open key (c), and the open key (a) of a program supplier is recognized (S2). Information obtained by decoding ciphering information (a) by the open key (a) and a password algorithm corresponding to the identifier (a) of the password algorithm is compared with the hash value of a program in order to decided whether the program is falsified or not after it has been supplied (S3). Proof information (b) is verified by the open key (c), and the open key (b) of an inspection organization inspecting the operation of the program is recognized (S4). Information obtained by decoding ciphering information (b) by the open key (b) and the password algorithm corresponding to identification information (b) of the password algorithm is compared with the hash value of the program in order to decide whether the program is falsified or not after the operation has been inspected (S5).



LEGAL STATUS

[Date of request for examination] 13.08.2002
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－339153
（P2000－339153A）
(43)公開日　平成12年12月８日(2000.12.8)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０６Ｆ　9/06	５５０	Ｇ０６Ｆ　9/06	５５０Ｅ　５Ｂ０７６
			５５０Ｚ

審査請求　未請求　請求項の数３　ＯＬ　（全８頁）

(21)出願番号　特願平11－145517

(22)出願日　平成11年５月25日(1999.5.25)

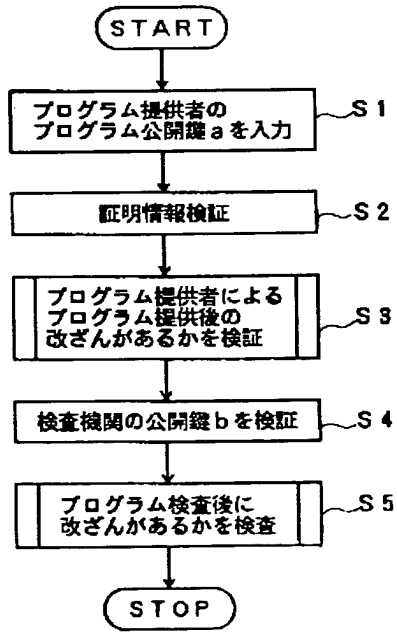
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　鈴木　勝彦
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　庭野　栄一
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100070150
弁理士　伊東　忠彦

最終頁に続く

(54)【発明の名称】　プログラム検証方法及び装置及びプログラム検証プログラムを格納した記憶媒体

(57)【要約】　（修正有）
【課題】　プログラム提供者のプログラム提供後、また検査機関のプログラム動作の検査後にプログラム改竄がないかの検証を行う。
【解決手段】　プログラムファイルと、証明機関の証明情報を検証するための公開鍵ｃが与えられると、公開鍵ｃにより証明情報ａを検証し、公開鍵ａがプログラム提供者の公開鍵であることを証明し、暗号化情報ａを公開鍵ａと暗号アルゴリズムの識別子ａに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較し、プログラム提供者の提供後にプログラムの改竄が行われていないかの検出を行い、公開鍵ｃにより証明情報ｂを検証することにより、公開鍵ｂがプログラムの動作を検査した検査機関の公開鍵であることを証明し、暗号化情報ｂを公開鍵ｂと暗号アルゴリズムの識別情報ｂに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較し、プログラムの動作を検査した後に、該プログラムの改竄が行われていないかの検出を行う。

本発明の原理を説明するための図



【特許請求の範囲】
【請求項１】　コンピュータの制御を記述したプログラムを検証するプログラム検証方法において、
検証の対象のプログラムと、該プログラムのハッシュ値をプログラム提供者のみが知る提供者秘密鍵ａで暗号化した暗号化情報ａと、該暗号化情報ａを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報ａと、該暗号化情報ａを復号するための公開鍵ａと証明機関が発行した公開鍵ａに対するお墨付きを示す証明情報ａと、プログラムのハッシュ値をプログラムの動作を検査した検査機関のみが知る検査機関秘密鍵ｂで暗号化した暗号化情報ｂと、該暗号化情報ｂを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報ｂと、該暗号化情報ｂを復号するための公開鍵ｂと該証明機関が発行した公開鍵ｂに対するお墨付きを示す証明情報ｂからなるプログラムファイルと、証明機関のお墨付きを示す情報を検証するための公開鍵ｃが与えられると、
前記公開鍵ｃにより前記証明情報ａを検証し、前記公開鍵ａが前記プログラム提供者の公開鍵であることを証明し、
前記暗号化情報ａを前記公開鍵ａと暗号アルゴリズムの識別子ａに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較し、前記プログラム提供者がプログラムを提供した後にプログラムの改竄が行われていないかの検出を行い、
前記公開鍵ｃにより前記証明情報ｂを検証することにより、前記公開鍵ｂがプログラムの動作を検査した検査機関の公開鍵であることを証明し、
前記暗号化情報ｂを前記公開鍵ｂと暗号アルゴリズムの識別情報ｂに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較し、前記プログラムの動作を検査した後に、該プログラムの改竄が行われていないかの検出を行うことを特徴とするプログラム検索方法。
【請求項２】　コンピュータの制御を記述したプログラムを検証するプログラム検証方法において、
検証の対象のプログラムと、該プログラムのハッシュ値をプログラム提供者のみが知る提供者秘密鍵ａで暗号化した暗号化情報ａと、該暗号化情報ａを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報ａと、該暗号化情報ａを復号するための公開鍵ａと証明機関が発行した公開鍵ａに対するお墨付きを示す証明情報ａと、プログラムのハッシュ値をプログラムの動作を検査した検査機関のみが知る検査機関秘密鍵ｂで暗号化した暗号化情報ｂと、該暗号化情報ｂを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報ｂと、該暗号化情報ｂを復号するための公開鍵ｂと該証明機関が発行した公開鍵ｂに対するお墨付きを示す証明情報ｂからなるプログラムファイルと、
前記プログラムファイルと、証明機関のお墨付きを示す情報を検証するための公開鍵ｃを入力する入力手段と、
前記公開鍵ｃにより前記証明情報ａを検証する手段と、
前記公開鍵ａが前記プログラム提供者の公開鍵であることを証明する手段と、前記暗号化情報ａを前記公開鍵ａと暗号アルゴリズムの識別子ａに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較する手段と、前記プログラム提供者がプログラムを提供した後にプログラムの改竄が行われていないかの検出を行う手段とを有するプログラム提供者検証手段と、
前記公開鍵ｃにより前記証明情報ｂを検証することにより、前記公開鍵ｂがプログラムの動作を検査した検査機関の公開鍵であることを証明する手段と、前記暗号化情報ｂを該公開鍵ｂと暗号アルゴリズムの識別情報ｂに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較する手段と、前記プログラムの動作を検査した後に、該プログラムの改竄が行われていないかの検出を行う手段とを有する検査機関検証手段とを有することを特徴とするプログラム検索装置。
【請求項３】　コンピュータの制御を記述したプログラムを検証するプログラム検証プログラムを格納した記憶媒体であって、
検証の対象のプログラムと、該プログラムのハッシュ値をプログラム提供者のみが知る提供者秘密鍵ａで暗号化した暗号化情報ａと、該暗号化情報ａを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報ａと、該暗号化情報ａを復号するための公開鍵ａと証明機関が発行した公開鍵ａに対するお墨付きを示す証明情報ａと、プログラムのハッシュ値をプログラムの動作を検査した検査機関のみが知る検査機関秘密鍵ｂで暗号化した暗号化情報ｂと、該暗号化情報ｂを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報ｂと、該暗号化情報ｂを復号するための公開鍵ｂと該証明機関が発行した公開鍵ｂに対するお墨付きを示す証明情報ｂからなるプログラムファイルと、証明機関のお墨付きを示す情報を検証するための公開鍵ｃを入力させる入力プロセスと、
前記公開鍵ｃにより前記証明情報ａを検証するプロセスと、前記公開鍵ａが前記プログラム提供者の公開鍵であることを証明するプロセスと、前記暗号化情報ａを前記公開鍵ａと暗号アルゴリズムの識別子ａに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較するプロセスと、前記プログラム提供者がプログラムを提供した後にプログラムの改竄が行われていないかの検出を行うプロセスとを有するプログラム提供者検証プロセスと、
前記公開鍵ｃにより前記証明情報ｂを検証することにより、前記公開鍵ｂがプログラムの動作を検査した検査機関の公開鍵であることを証明するプロセスと、前記暗号化情報ｂを該公開鍵ｂと暗号アルゴリズムの識別情報ｂ

に対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較するプロセスと、前記プログラムの動作を検査した後に、該プログラムの改竄が行われていないかの検出を行うプロセスとを有する検査機関検証プロセスとを有することを特徴とするプログラム検索プログラムを格納した記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、プログラム検証方法及び装置及びプログラム検証プログラムを格納した記憶媒体に係り、特に、プログラム提供者がプログラムを提供した後に行われたプログラムの改竄の検出、検査機関がプログラムの動作を検査した後に行われたプログラムの改竄の検出を行うためのプログラム検証方法及び装置及びプログラム検証プログラムを格納した記憶媒体に関する。

【０００２】

【従来の技術】従来、情報提供者が情報Ａと当該情報Ａのハッシュ値を当該情報Ａの情報提供者のみが知る秘密鍵で暗号化した暗号化情報Ｂと、暗号化情報Ｂを復号するための公開鍵と証明機関の公開鍵に対するお墨付きを示す証明情報Ｃを組として配布し、その配布された情報（Ｂ＋Ｃ）を受け取った利用者が、暗号化情報Ｂを公開鍵により復号した復号情報Ｄと元の情報Ａのハッシュ値とを比較することで、情報提供者が情報Ａを提供した後に情報の改竄が行われていないかを検証する方法がある。

【０００３】

【発明が解決しようとする課題】しかしながら、上記従来の情報の配布方法でプログラムを配布した場合、プログラム提供者がプログラムを提供した後、プログラムが改竄されていないかの検証は可能であるが、プログラムを実行した場合、プログラムが不正な動作をするかの識別は不可能である。

【０００４】本発明は、上記の点に鑑みなされたもので、プログラム提供者がプログラムを提供した後、プログラムが改竄されていないかの検証と、検査機関がプログラムの動作の検査をした後に行われたプログラムが改竄されていないかの検証を行うことにより、提供されたプログラムが安全に動作することを証明することが可能なプログラム検証方法及び装置及びプログラム検証プログラムを格納した記憶媒体を提供することを目的とする。

【０００５】

【課題を解決するための手段】図１は、本発明の原理を説明するための図である。本発明（請求項１）は、コンピュータの制御を記述したプログラムを検証するプログラム検証方法において、検証の対象のプログラムと、該プログラムのハッシュ値をプログラム提供者のみが知る提供者秘密鍵ａで暗号化した暗号化情報ａと、該暗号化情報ａを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報ａと、該暗号化情報ａを復号するための公開鍵ａと証明機関が発行した公開鍵ａに対するお墨付きを示す証明情報ａと、プログラムのハッシュ値をプログラムの動作を検査した検査機関のみが知る検査機関秘密鍵ｂで暗号化した暗号化情報ｂと、該暗号化情報ｂを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報ｂと、該暗号化情報ｂを復号するための公開鍵ｂと該証明機関が発行した公開鍵ｂに対するお墨付きを示す証明情報ｂからなるプログラムファイルと、証明機関のお墨付きを示す情報を検証するための公開鍵ｃが与えられると（ステップ１）、公開鍵ｃにより証明情報ａを検証し、公開鍵ａがプログラム提供者の公開鍵であることを証明し（ステップ２）、暗号化情報ａを公開鍵ａと暗号アルゴリズムの識別子ａに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較し、プログラム提供者がプログラムを提供した後にプログラムの改竄が行われていないかの検出を行い（ステップ３）、公開鍵ｃにより証明情報ｂを検証することにより、公開鍵ｂがプログラムの動作を検査した検査機関の公開鍵であることを証明し（ステップ４）、暗号化情報ｂを公開鍵ｂと暗号アルゴリズムの識別情報ｂに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較し、プログラムの動作を検査した後に、該プログラムの改竄が行われていないかの検出を行う（ステップ５）。

【０００６】図２は、本発明の原理構成図である。本発明（請求項２）は、コンピュータの制御を記述したプログラムを検証するプログラム検証方法において、検証の対象のプログラムと、該プログラムのハッシュ値をプログラム提供者のみが知る提供者秘密鍵ａで暗号化した暗号化情報ａと、該暗号化情報ａを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報ａと、該暗号化情報ａを復号するための公開鍵ａと証明機関が発行した公開鍵ａに対するお墨付きを示す証明情報ａと、プログラムのハッシュ値をプログラムの動作を検査した検査機関のみが知る検査機関秘密鍵ｂで暗号化した暗号化情報ｂと、該暗号化情報ｂを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報ｂと、該暗号化情報ｂを復号するための公開鍵ｂと該証明機関が発行した公開鍵ｂに対するお墨付きを示す証明情報ｂからなるプログラムファイル１と、プログラムファイル１と、証明機関のお墨付きを示す情報を検証するための公開鍵ｃを入力する入力手段２と、公開鍵ｃにより証明情報ａを検証する手段と、公開鍵ａがプログラム提供者の公開鍵であることを証明する手段と、暗号化情報ａを公開鍵ａと暗号アルゴリズムの識別子ａに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較する手段と、プログラム提供者がプログラムを提供した後にプログラムの改竄が行われてい

ないかの検出を行う手段とを有するプログラム提供者検証手段３と、公開鍵ｃにより証明情報ｂを検証することにより、公開鍵ｂがプログラムの動作を検査した検査機関の公開鍵であることを証明する手段と、暗号化情報ｂを該公開鍵ｂと暗号アルゴリズムの識別情報ｂに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較する手段と、プログラムの動作を検査した後に、該プログラムの改竄が行われていないかの検出を行う手段とを有する検査機関検証手段４とを有する。

【０００７】本発明（請求項３）は、コンピュータの制御を記述したプログラムを検証するプログラム検証プログラムを格納した記憶媒体であって、検証の対象のプログラムと、該プログラムのハッシュ値をプログラム提供者のみが知る提供者秘密鍵ａで暗号化した暗号化情報ａと、該暗号化情報ａを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報ａと、該暗号化情報ａを復号するための公開鍵ａと証明機関が発行した公開鍵ａに対するお墨付きを示す証明情報ａと、プログラムのハッシュ値をプログラムの動作を検査した検査機関のみが知る検査機関秘密鍵ｂで暗号化した暗号化情報ｂと、該暗号化情報ｂを生成するために利用したハッシュアルゴリズムと暗号アルゴリズムの識別情報ｂと、該暗号化情報ｂを復号するための公開鍵ｂと該証明機関が発行した公開鍵ｂに対するお墨付きを示す証明情報ｂからなるプログラムファイルと、証明機関のお墨付きを示す情報を検証するための公開鍵ｃを入力させる入力プロセスと、公開鍵ｃにより証明情報ａを検証するプロセスと、公開鍵ａがプログラム提供者の公開鍵であることを証明するプロセスと、暗号化情報ａを公開鍵ａと暗号アルゴリズムの識別子ａに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較するプロセスと、プログラム提供者がプログラムを提供した後にプログラムの改竄が行われていないかの検出を行うプロセスとを有するプログラム提供者検証プロセスと、公開鍵ｃにより証明情報ｂを検証することにより、公開鍵ｂがプログラムの動作を検査した検査機関の公開鍵であることを証明するプロセスと、暗号化情報ｂを該公開鍵ｂと暗号アルゴリズムの識別情報ｂに対応した暗号アルゴリズムで復号した情報とプログラムのハッシュ値を比較するプロセスと、プログラムの動作を検査した後に、該プログラムの改竄が行われていないかの検出を行うプロセスとを有する検査機関検証プロセスとを有する。

【０００８】上記のように、本発明によれば、プログラム提供者がプログラムを提供した後に行われたプログラムの改竄を検出するのみならず、検査機関がプログラムの動作を検査した後に行われた当該プログラムの改竄の双方を検出することが可能となる。

【０００９】

【発明の実施の形態】図３は、本発明のシステム構成を示す。同図に示すシステムは、ＩＣチップ１０、端末２０及び証明機関サーバ３０から構成され、端末２０と証明機関サーバ３０とがネットワークで接続されている。

【００１０】以下では、本発明の動作を行うコンピュータをＩＣチップとして説明する。図４は、本発明のＩＣチップの構成を示す。ＩＣチップ１０は、端末２０と通信を行うための入出力インタフェース１３、情報を格納するためのメモリ１１、メモリ１１に格納された情報の演算を行うプロセッサ１２からなり、１つのチップで構成される。

【００１１】プロセッサ１２は、ハッシュ生成部１２１、署名復号部１２２、及びデータ比較部１２３から構成される。ハッシュ生成部１２１は、ＭＤ５，ＳＨＡ等の暗号アルゴリズム識別情報とプログラム等のデータを入力とし、当該データのハッシュを生成する。署名復号部１２２は、ＲＳＡ，ＥＳＩＧＮ等の暗号アルゴリズム識別情報と暗号化された暗号化データを入力とし、当該暗号アルゴリズム識別情報と暗号化データを復号する。

【００１２】データ比較部１２３は、ハッシュ生成部１２１で生成されたハッシュ値と署名復号部１２で復号された復号データとを比較する。図５は、本発明の端末の構成を示す。端末２０は、ＩＣチップ１０の制御を行うためのプログラムファイルを格納するためのメモリ２１とＩＣチップ１０と通信を行うための入出力インタフェース２２とを有する。また、ネットワークにより証明機関サーバ３０からの証明機関の公開鍵を取得する機能を有する。

【００１３】メモリ２１には、プログラムと、署名ａ，暗号アルゴリム識別子ａ、証明書ａの組と、署名ｂ，暗号アルゴリム識別子ｂ、証明書ｂの２つの組が格納されている。秘密鍵ａは、当該プログラムの提供者のみが知るＲＳＡ、ＥＳＩＧＮ等の署名アルゴリズムの秘密鍵である。

【００１４】署名ａは、ＭＤ５等のハッシュアルゴリズムにより生成してプログラムのハッシュ値を入力とし、ＲＳＡ，ＥＳＩＧＮ等の署名アルゴリズムにより生成した署名である。暗号アルゴリズム識別子ａは、署名ａを生成するために利用した署名アルゴリズムとハッシュアルゴリズムを示す暗号アルゴリズム識別子である。

【００１５】証明書ａは、秘密鍵ａと対である公開鍵ａに対するお墨付き情報であるＯＳＩのＸ．５０９に従った証明書である。署名ｂは、プログラムの動作を検査した検査機関のみが知るＲＳＡ，ＥＳＩＧＮ等の署名アルゴリズムの秘密鍵ｂとＭＤ５，ＳＨＡ等のハッシュアルゴリズムにより生成したプログラムのハッシュ値を入力とし、ＲＳＡ，ＥＳＩＧＮ等の署名アルゴリズムにより生成した署名である。

【００１６】暗号アルゴリズム識別子ｂは、署名ｂを生成するために利用した署名アルゴリズムとハッシュアルゴリズムを示す識別子である。証明書ｂは、秘密鍵ｂで

対である公開鍵ｂに対するお墨付き情報であるＯＳＩのＸ．５０９勧告に従って作成された証明書である。端末２０は、最初に、ネットワークにより接続された証明機関サーバ３０から証明機関が発行する公開鍵を取得し、入出力インタフェース２２によりＩＣチップ１０に転送する。

【００１７】次に、端末２０のメモリ２１に格納されているプログラムファイル２１１を読み出し、入出力インタフェース２２によりＩＣチップ１０に転送する。次に、ＩＣチップ１０の入出力インタフェース１３において、端末２０から転送された公開鍵及びプログラムファイルを取得して、メモリ１１に格納する。これにより、図５に示されるプログラムファイル２１１の内容が当該メモリ１１に格納されることになる。これにより、プロセッサ１２では、当該メモリ１１に格納されたプログラムファイルを読み込んで処理を行う。

【００１８】本発明の検証の方法を以下に示す。図６は、本発明のプログラム提供後の改竄を検証する処理のフローチャートである。

ステップ１０１）　ＩＣチップ１０のプロセッサ１２は、メモリ１１に格納されたプログラムファイルに含まれる証明書ａをＯＳ１のＸ－５０９勧告に従い検証する。

【００１９】詳しくは、

①　メモリ１１に格納されたプログラムファイル中の証明書ａに対する署名情報を除く証明書ａの情報と証明書ａに含まれる署名アルゴリズム情報を入力とし、ハッシュ生成部１２１により、対応する暗号アルゴリズムにより演算を実行し、ハッシュ値Ａを生成する。

【００２０】②　署名復号部１２２において、メモリ１１に格納された証明機関の公開鍵と証明書ａに対する署名情報と証明書ａに含まれる署名アルゴリズム情報を入力とし、対応する暗号アルゴリズムにより演算を実行し、復号された復号情報Ａを生成する。

③　データ比較部１２３は、生成したハッシュ値Ａと復号された復号情報Ａを入力とし、双方の比較を行い、一致すれば、証明機関が証明書ａを発行した後に、証明書ａが第三者により改竄されていないことが保証される。

【００２１】ステップ１０２）　次に、証明書ａの改竄が検出されない場合、署名ａの検証を行う。

ステップ１０３）　メモリ１１に格納されたプログラムと署名ａの生成に利用した暗号アルゴリズム識別子ａを入力とし、ハッシュ生成部１２１により対応する暗号アルゴリズムにより演算を実行し、プログラムのハッシュ値Ｃを生成する。

【００２２】ステップ１０４）　メモリ１１に格納された署名ａと証明書ａに含まれる公開鍵ａと暗号アルゴリズム識別子を入力とし、署名復号部１２２で対応する暗号アルゴリズムにより演算を実行し、復号された復号情報Ｃを生成する。

ステップ１０５）　次にデータ比較部１２３において、ハッシュ生成部１２１で生成されたハッシュ値Ｃと復号情報Ｃを入力とし、データの比較を行う。

【００２３】ステップ１０６）　比較した結果が一致すれば、プログラム提供者がプログラムを提供した後に、第三者によるプログラムが改竄されていないことが証明される。次に、上記の処理に引き続いて、検査機関のプログラム動作の検査後におけるプログラムの改竄を検証する動作を説明する。

【００２４】図７は、本発明の検査機関のプログラム動作の検査後の改竄を検証する処理のフローチャートである。

ステップ２０１）　プログラムの動作の検査機関の証明書ｂを公開鍵ｃにより検証することにより、公開鍵ｂがプログラムの動作を検査した検査機関の公開鍵であることを証明を検証する。検証方法は、前述の図６のフローチャートのステップ１０１と同様である。

【００２５】ステップ２０２）　証明書ｂの改竄が検出されない場合には、証明書ｂは正規ものとする。

ステップ２０３）　証明書ｂが正規である場合には、メモリ１１に格納されたプログラムと署名ｂの生成に利用した暗号アルゴリズム識別子ｂを入力とし、ハッシュ生成部１２１により対応する暗号アルゴリズムにより演算を実行し、プログラムのハッシュ値Ｄを生成する。

【００２６】ステップ２０４）　メモリ１１に格納された署名ｂと証明書ｂに含まれる公開鍵ｂと暗号アルゴリズム識別子を入力とし、署名復号部１２２で対応する暗号アルゴリズムにより演算を実行し、復号された復号情報Ｄを生成する。

ステップ２０５）　次にデータ比較部１２３において、ハッシュ生成部１２１で生成されたハッシュ値Ｄと復号情報Ｄを入力とし、データの比較を行う。

【００２７】ステップ２０６）　比較した結果が一致すれば、検査機関がプログラムの動作を検査した後に、第三者によるプログラムが改竄されていないことが証明される。また、上記の例では、図４の構成に基づいて説明しているが、ＩＣチップに限定されることなく、パソコン等で行うようにしてもよい。また、図６と図７の処理を別々のプロセッサで行うようにしてもよい。

【００２８】また、上記の図６、図７に示す検証処理をプログラムとして構築し、ＩＣメモリ、ディスク装置や、フロッピーディスクやＣＤ－ＲＯＭ等の可搬記憶媒体に格納しておき、本発明を実施する際にインストールすることにより、容易に本発明を実現できる。なお、本発明は、上記の例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【００２９】

【発明の効果】上述のように、本発明によれば、プログラム提供者がプログラムを提供した後に行われた改竄を検出するのみならず、検査機関がプログラムの動作を検

査した後に行われたプログラムの改竄も検出することが可能であるため、提供されたプログラムが安全に動作することを証明することができる。

【図面の簡単な説明】

【図１】本発明の原理を説明するための図である。

【図２】本発明の原理構成図である。

【図３】本発明のシステム構成図である。

【図４】本発明のＩＣチップの構成図である。

【図５】本発明の端末の構成図である。

【図６】本発明のプログラム提供後の改竄を検証する処理のフローチャートである。

【図７】本発明の検査機関のプログラム動作の検査後の改竄を検証する処理のフローチャートである。

【符号の説明】

１　プログラムファイル

２　入力手段

３　プログラム提供者検証手段

４　検証機関検証手段

１０　ＩＣチップ

１１　メモリ

１２　プロセッサ

１３　入出力インタフェース

２０　端末

３０　証明機関サーバ

２１　メモリ

２２　入出力インタフェース

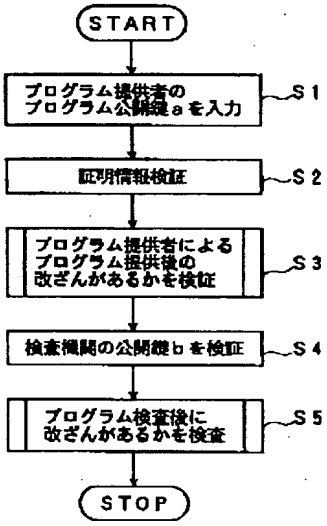
１２１　ハッシュ生成部

１２２　署名復号部

１２３　データ比較部

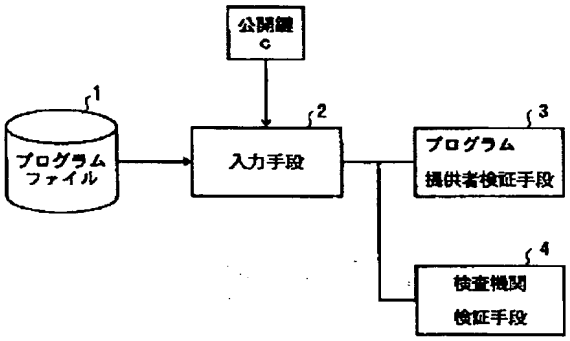
【図１】

本発明の原理を説明するための図



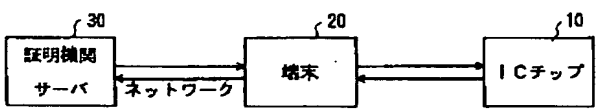
【図２】

本発明の原理構成図



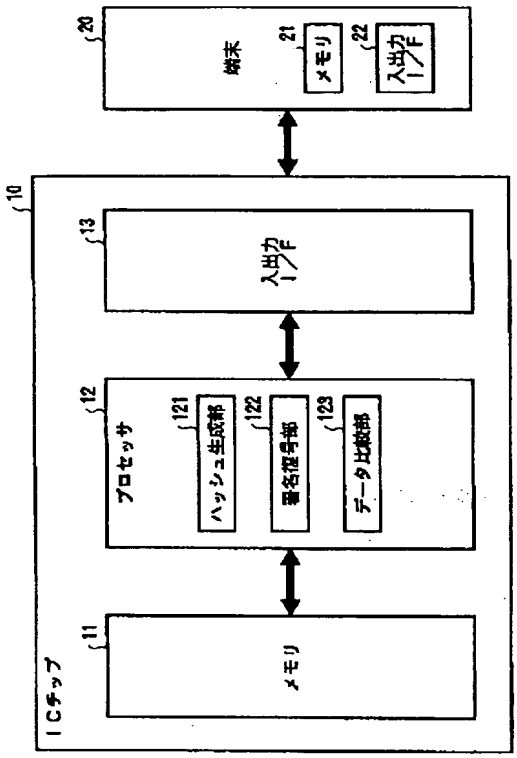
【図３】

本発明のシステム構成図



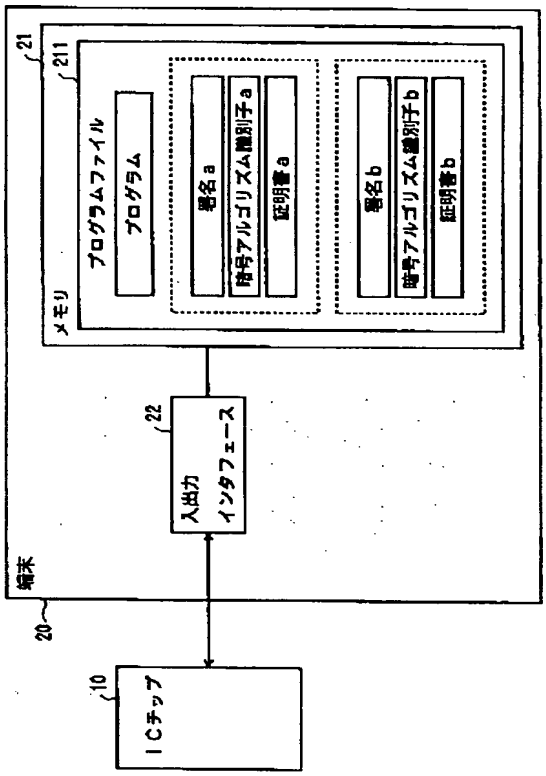
【図４】

本発明のＩＣチップの構成図



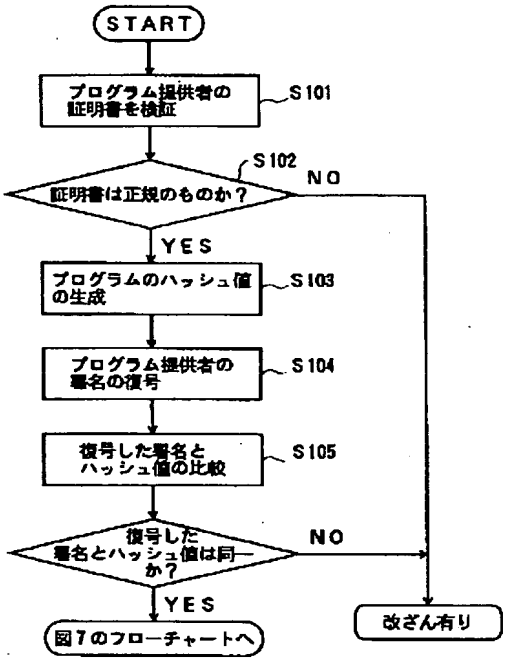
【図５】

本発明の端末の構成図



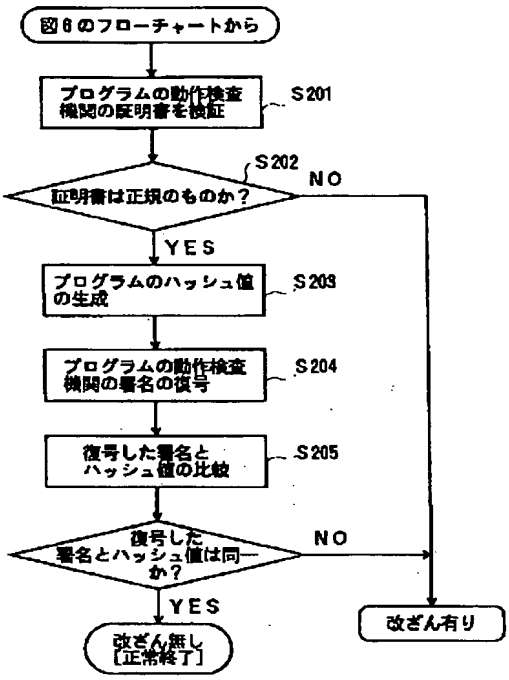
【図６】

本発明のプログラム提供後の
改ざんを検証する処理のフローチャート



【図７】

本発明の検査機関のプログラム動作の検査後の
改ざんを検証する処理のフローチャート



フロントページの続き

(72)発明者　千葉　伸浩
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　細田　泰弘
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

Ｆターム(参考)　5B076 FA13 FA14